A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants.	Case No. 04-1199-SLR **[CONTAINS CONFIDENTIAL INFORMATION]**

REBUTTAL EXPERT REPORT OF STEPHEN E. SMAHA

I may be called to testify at trial to rebut expert testimony offered about the opinions set forth by Dr. George Kesidis in his April 28, 2006 report. Toward that end, I incorporate my April 21, 2006 expert report.

I. QUALIFICATIONS

My qualifications are set forth in detail in my April 21, 2006 expert report.

8. User-defined policy for bandwidth profiles: For manually configured Internet address regions, see if current traffic rates over the most recent 2 minutes exceed the past historical traffic rates since the device was last started by more than 5 standard deviations. (Dawson 2006) (Song/Jahanian)

Alerts created based on these heuristics are formatted into ISS event messages in ASCII format and transmitted to the ISS SiteProtector. In addition, the Analyzer may be manually configured to provide passive host discovery information to SiteProtector. In this option, the Analyzer sends a message to SiteProtector for each Internet address that appears in network traffic that had not previously been seen. Also, the Analyzer sends "heartbeat" messages at regular intervals to the SiteProtector to provide an indication of the integrity of the sensor's functions.

The Collectors and Analyzers are manually configured by users communicating directly using Web browsers. The SiteProtector itself does not control or otherwise communicate with the Collectors and Analyzers.

b. PNADS Does Not Infringe '338

Please refer to my April 21, 2006 expert report for an overview of the claims of the '338 patent.

'338 Claim 1. This patent requires a method of network surveillance that includes "receiving network packets handled by a network entity".

However, as described above, in this system the PNADS Collector and Analyzer devices themselves process NetFlow records originating in the router/switch, and not the stream of network user data packets that are themselves handled by the router/switch. In standalone mode, the NetFlow information is generated from network packets retrieved from a tap. Therefore

PNADS does not "receive network packets handled by a network entity". In this case the network surveillance is performed by the router/switch.

None of the activities of the PNADS Collector resemble "building at least one long-term and at least one short-term statistical profile" ('338, Claim 1). Concerning the PNADS Analyzer, of the eight heuristics described above, only #8 ("User-defined policy for bandwidth profiles") requires examination.

According to (Song/Jahanian), the PNADS device by default does not enable heuristic #8 when the device is installed on a customer network. To enable this heuristic, the customer specifies one or more groups of Internet addresses to be profiled as a collective group of sources and destinations of network traffic. This collection of sources and destinations is called a "traffic filter", and it is treated as an aggregate. The PNADS device itself is not capable of creating, maintaining, or using bandwidth profiles for general and arbitrary network traffic to or from arbitrary Internet addresses, unlike the system described in the patent specification.

PNADS heuristic #8 is implemented by creating and maintaining 4 baselines for each configured traffic filter. For each traffic filter, PNADS stores the mean and standard deviation of the number of bytes and packets in the current (2 minute) history record, and the same information for the most recent Day, Week, and Continuous, where each baseline profile consists of a static number of 30 minute time bins per timeframe (1 for Continuous, 48 for Day, and 336 for Week). At the end of the current day, the Day data is averaged into the Week data on a time-proportional basis. Similarly, the Week is averaged into Month, and so on. The detection method compares the the current (last 2 minutes) data for a given address group with the weighted sum of the values of the Day/Week/Continuous data, where the weights employed are

fixed in the system and are not historically adaptive like those in the patent specification. If the current data exceeds the static threshold weighted sum, heuristic #8 generates an alert.

The PNADS heuristic #8 feature was found at Arbor to be somewhat useful for finding disruptions among high bandwidth stable aggregates of computers (like a Bloomberg financial data feed or manufacturing data going to a corporate server), but to be ineffective for performing analyses of traffic created by human users of enterprise networks, because the latter case has high false positive alarm rates.

SRI's eStat, in its implementation of the algorithm, suffered from the same inherent problem. SRI replaced it with an entirely new engine in more recent versions of its EMERALD software.

In my opinion heuristic #8 does not perform the step of "determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity." Under the ISS claim construction this means "determining whether the difference between the short-term statistical profile and long-term statistical profile exceeds a threshold that is empirically determined to indicate suspicious activity based on the historically adaptive deviation between the two profiles, requiring no prior knowledge of suspicious activity." I agree with the ISS claim construction because the terms used in the patent claims by themselves do not suggest a meaning, and so I have examined the patent's specification for guidance. The patent specification describes performing a historically adaptive analysis of deviations of behavior from the long-term profile to make the determination of what is suspicious. SRI's construction does not provide guidance as to how to decide which monitored activities are suspicious, and therefore one skilled in the art could not determine what the claim means from that construction.

I note that PNADS Analyzer in this mode reports changes in the last two minutes of network traffic compared to a fixed percentage value times the weighted values from previously recorded baselines. (Song/Jahanian) This does not constitute use of a "historically adaptive" deviation between short-term and long-term profiles, because the amount of required deviation is fixed and does not change. Nor does it use a non-parametric statistical model, per the patent specification. Rather, the PNADS method uses a fixed threshold to compare the short-term and long-term profiles, and this is neither historically adaptive nor empirically determined. These two distinctions are substantially different from the method described in the patent; the patent specification emphasizes the importance of non-parametric empirical distinctions ('338, Col 6, 52-58) in detecting intrusive or exceptional activity.

I understand that if an independent claim is not infringed, then neither are any claims that depend on it. Therefore claims 4, 5, 11-13, and 15-19 are not infringed. I addition these claims are not infringed for further reasons as discussed below.

'338 Claim 4. PNADS does not itself "monitor data transfers by monitoring network packet data transfer volume", since it is processing NetFlow records, and not by itself monitoring network packet data in order to derive its volume. In addition, the byte counts created in the PNADS Collector's START/UPDATE/END records described above do not themselves indicate the data transfers between addresses, since the byte counts cover all bytes transferred, including the header information, and are not limited to the network packet data portions (the so-called "payloads").

'338 Claim 5. PNADS does not itself "monitor data network connections by monitoring network connection requests", since it is processing NetFlow records reporting on connections that have already been established, rather than requested.

'338 Claim 11. PNADS event reporting does not violate this claim because, per my response to '338 Claim 1 above, it simply provides a report that an exception to a user-defined policy has occurred, and this policy itself could be established for non-security-related reasons.

'338 Claim 12. When the PNADS device provides an event report to the ISS SiteProtector, this does not constitute "transmitting an event to a network monitor" because the ISS SiteProtector does not itself constitute a "monitor" as intended in '338 as discussed above.

'338 Claim 13. When the PNADS device provides an event report to the ISS SiteProtector, this does not constitute "transmitting an event to a hierarchically higher network monitor" because the ISS SiteProtector does not itself constitute a "monitor" as intended in '338, for the reasons stated above. Moreover, PNADS does not constitute a monitor. It is not made up of generic code that can be dynamically configured and reconfigured with reusable modules, as required of a monitor.

'338 Claim 18. My response to this claim is same as to '338 Claim 1.

'338 Claim 19. My response to this claim is same as to '338 Claim 1.

'338 Claim 24. My response to this claim is same as to '338 Claim 1.

VII. Reservation of rights

I reserve the right to amend or supplement this statement based on further discovery and preparation in this action, including my review of any expert statement submitted on behalf of SRI or Symantec.

Dated: 16 May 2006

Stephen E. Smaha